

The New York Times |

Opinion

Editorial Observer; Rolling Down the Highway, Looking Out for Flawed Elections

By ADAM COHEN AUG. 8, 2004

The elections director of Mohave County, Ariz., was so proud of his new electronic voting system that Bev Harris barely had the heart to point out its vulnerabilities. But she did, and before long she was ticking off the ways that she said an outsider could hijack his central tabulator -- the computer that stores all of the county's votes -- and steal an election.

By the time she had shown him a "backdoor" way to gain access to his software without a password, the elections director was visibly concerned. Before she left, he asked her to send him a list of things he could do to safeguard this year's election.

Ms. Harris's visit to Mohave County was part of a monthlong trip in which she and her deputy, Andy Stephenson, traveled to 10 states, investigating flaws in electronic voting and giving on-the-fly computer security tutorials.

The trip started out in Ohio, where they knocked on the doors of employees of Diebold, one of the largest and most criticized voting machine companies. It ended in late July in Las Vegas at Defcon, a hackers' convention, where the consensus was that cracking a voting machine might not be so hard.

Ms. Harris, the director of Black Box Voting (the Web address is www.blackboxvoting.org), has made herself public enemy No.1 for voting machine manufacturers, and some elections officials, with her hard-edged attacks on

electronic voting and her investigative style. (She acknowledges that at one point in Ohio, she and Mr. Stephenson hid in the bushes with a microphone, eavesdropping on Diebold workers.)

But there is no denying that Ms. Harris, a onetime literary publicist from the Seattle area, is responsible for digging up some of the most disturbing information yet to surface about the accuracy and integrity of electronic voting.

"I wouldn't want to play her role," says Aviel Rubin, a Johns Hopkins computer science professor and a leading critic of electronic voting. "But we're all better off that she's out there."

When they're in road-trip mode, Ms. Harris and Mr. Stephenson are a high-tech public-interest group on wheels. With a laptop computer connected to the Internet by cellphone, they toggle between MapQuest, hunting down directions, and Google, searching for the latest electronic voting information. The phone rings frequently with leads to be investigated. As they drove through San Bernardino, Calif., Ms. Harris took a call from a small-town official in Indiana, who claimed a voting machine salesman picked up a top elections official in his county in a limousine and took her on a shopping spree.

In the San Bernardino County elections office, Ms. Harris asked the registrar of voters to explain why, in the presidential primary in March, the vote totals went down in the days after the election. He explained that the county's electronic voting system had faulty software that accidentally held on to some test votes, and added them to the real votes that were cast. He insists that the story showed that the system worked well, since the extra votes were eventually found. Ms. Harris is skeptical.

Even many of Ms. Harris's detractors concede that her past investigations have shaken up the electronic voting field.

While surfing the Internet last year, she came across secret source code -- programming instructions -- for Diebold voting machines, and made it publicly available. Mr. Rubin relied on the code she found in a report last July in which he identified what he called "stunning, stunning flaws" in Diebold software.

Ms. Harris also found software updates, or patches, that Diebold added to Georgia's electronic voting machines before the 2002 election, even though the software had not been properly certified. More recently, she caused waves in King County, Wash., her home county, when she revealed that one of the main designers of its elections management computer system was a convicted felon, who had embezzled \$465,361 from a Seattle law firm.

Ms. Harris worries a lot about this year's election. One of the key vulnerabilities, she says, is the central tabulator, which could control a million or more votes in some counties. There will be thousands of election workers -- including temporaries who may not even have had their backgrounds checked -- with access to these computers, who she believes could change vote totals rapidly. "It isn't hacking an election," she says. "It's editing an election." She and many computer scientists worry that modems on the machines will make them vulnerable.

Ms. Harris hopes to expand her small Black Box Voting organization into a consumer-protection agency for electronic voting and election procedures.

There is clearly a need. When electronic voting was rolled out, with even less security than is in place now, groups like the League of Women Voters and the American Civil Liberties Union did little to warn about the dangers, and large public interest organizations and foundations are still doing too little.

The burden has been carried by a small group of public-minded citizens. Dr. Rebecca Mercuri of Harvard (www.notablessoftware.com), Prof. David Dill of Stanford University (www.verifiedvoting.org) and Professor Rubin have done heroic work in academia to investigate and explain electronic voting. Organizations like the Miami-Dade Election Reform Coalition, which found a significant flaw in the audit function in Florida voting machines, and the Computer Ate My Vote movement are also making a real difference.

For now, Ms. Harris is continuing to work her leads. She has to follow up on an e-mail message she picked up on the road in Arizona, from an elections judge in Santa Clara, Calif., saying there was a problem there. "Usually when it's an elections judge, it's something good," she says.

Most disturbing of all, she has heard reports that one of the big machine manufacturers may be including a modem connection between a county's tabulating computer and the manufacturer's own headquarters, which could allow it to change vote totals from afar.

"It's pretty much never-ending," Ms. Harris says with a sigh.